IN THE SPECIFICATION:

Please amend the specification as follows:

Please replace the first paragraph in the "Description of the Prior Art" section (Page 1, Lines 16-21) with the following amended paragraph:

The Secure Socket Layer (SSL) protocol (~~see The~~ e.g., SSL Protocol Version 3.0, ~~http://www.netscape.com/eng/ssl3/ssl-toc.html~~) is presently the *de facto* industry standard for Web security. In fact, because most E-commerce applications are based on the Web, the SSL protocol is built into almost all Web servers and browsers, such as Netscape Enterprise Server, Microsoft Web Server, Netscape Communicator, and Microsoft Internet Explorer (IE).

Please replace the first paragraph in the "Current or Known Solutions" section (Page 3, Line 19 – Page 4, Line 3) with the following amended paragraph:

The SSL protocol itself does not specify how the root CA certificate validation should be implemented. Thus, such implementation is very much vendor dependent and proprietary to each vendor. There are very few publications regarding to this issue. Some well-known implementations are Netscape Communicator and Microsoft IE, which are based on a certificate database embedded in the browser software. In March 2001, an IETF draft, the Simple Certificate Validation Protocol (SCVP~~; see Simple Certificate Validation Protocol, http://search.ietf.org/internet-drafts/draft-ietf-pkix-scvp06.txt~~) regarding such certificate validation was published. The proposed protocol is based on a server that performs certificate validation.

Please replace the paragraph on Page 14, Line 21 – Page 15, Line 9 with the following amended paragraph:

The preferred hash function can be either MD5 or SHA-1. For maximum security, SHA-1 is presently preferred. The ASN.1 (~~see~~ Abstract Syntax Notation, ~~ftp://ftp.rsa.com/pub/pkcs/ascii/layman.asc~~) definition of the TIO, which follows the PKCS#7 standard (~~see~~ e.g., The Public-Key Cryptography Standards (PKCS), RSA Data Security, Inc., Version 1.5, revised Nov. 1, 1993, ~~http://www.sasecurity.com/rsalabs/pkcs/pkcs-7/~~), and the semantics of each bit in the trust vector (TV) are described in greater detail below. Because the output of the hash function has a fixed length of twenty bytes maximum, i.e. when using SHA-1, and the TV is likely from one to two bytes, the size of the whole table is very small. Thus, the TIO readily fits into consumer devices, such as set-top boxes, cell phones, hand held computers, and pagers. For example, a TIO derived from 50 Root Certificates has the size of around 1 k. Furthermore, with a TIO containing the hash values of the most popular root CA certificates, clients are capable of communicating with the majority of the secure web sites.

Please replace the Abstract section with the following amended paragraph (amended to replace 2 paragraphs with 1 paragraph):

A unique TIO based trust information delivery scheme is disclosed that allows clients to verify received certificates and to control Java and Javascript access efficiently. This scheme fits into the certificate verification process in SSL to provide a secure connection between a client and a Web server. In particular, the scheme is well suited for incorporation into consumer devices that have a limited footprint, such as set-top boxes, cell phones, and handheld computers. Furthermore, the TIO update scheme disclosed herein allows clients to update certificates securely and dynamically.